Department of Homeland Security Daily Open Source Infrastructure Report for 12 July 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Department of Homeland Security with the cooperation of the Port Authority of New York and New Jersey will test and evaluate security equipment and operating procedures at the Exchange Place Port Authority−Trans Hudson Station from July 13−27, as part of the effort to protect citizens and critical infrastructure from possible terrorist attacks. (See item 11)

- The Associated Press reports at least 163 people were killed and 464 injured when blasts ripped apart commuter trains in the Indian city of Mumbai during evening rush hour on Tuesday, July 11. (See item 12)

- The New York Times reports New York City officials have offered a blueprint for identifying a flu pandemic outbreak, containing its spread, and distributing scarce resources like ventilators and antiviral medications. (See item 22)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 11, Associated Press* — **Producers work hard to squeeze energy out of rocks.** America's thirst for energy is forcing some of Oklahoma's biggest producers to look for natural gas in deposits of shale. Encouraged by the explosive growth of natural gas production in North

Texas' Barnett Shale, Chesapeake Energy Corporation and Devon Energy Corporation have entered new shale activity in Oklahoma and Arkansas. The Caney, the Woodford, and the Fayetteville shale formations, known to have large deposits of gas, could be as prolific as the Barnett Shale. The Barnett now produces about 1.2 billion cubic feet of gas a day.
Source: http://www.kten.com/Global/story.asp?S=5129310

2. *July 11, Energy Information Administration* — **Energy Information Administration: Short−Term Energy Outlook.** Summer 2006 (April 1 to September 30) regular gasoline pump prices are now expected to average $2.88 per gallon, 12 cents per gallon higher than last month's projection and 51 cents higher than last year's average of $2.37 per gallon. In 2006 and 2007, the West Texas Intermediate (WTI) crude oil spot price is projected to average about $69 per barrel. Natural gas prices are projected to be lower through the rest of this year relative to the corresponding period in 2005. Electricity consumption is expected to increase by 0.6 percent in 2006 and by 1.4 percent in 2007. Sharply higher prices for peaking fuels and high summer demand for those fuels, particularly natural gas, contributed to the increases in 2005. These same factors are expected to raise prices in 2006. Electric power sector consumption of coal is projected to grow by some 0.3 percent in 2006 and by another 1.6 percent in 2007.
Source: http://www.eia.doe.gov/steo

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *July 10, Associated Press* — **Wisconsin propane gas explosion leaves two missing, prompts highway closure.** A series of explosions damaged a cottage and two other buildings in a resort community in Wisconsin early Monday, July 10, sending seven people to hospitals. Two people were unaccounted for. The blasts struck a grocery store, a cottage and a maintenance building with a living quarters on the Door County peninsula, which juts into Lake Michigan. Charles Most, chairman of the Door County Board and the Liberty Grove Town Board, said investigators believe a propane gas leak might have triggered the explosion, though they had not yet pinpointed the cause. Highway 42 was closed as a result and authorities urged people to stay away from the area.
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=46&id=50162

[Return to top]

Defense Industrial Base Sector

4. *July 11, Aviation Week* — **IT industry issues warning on specialty metals proposal.** Major players in the U.S. information technology (IT) industry are warning that they will not be able to sell their commercial products to the Department of Defense (DoD) if House defense authorization language for fiscal 2007 becomes law. The language relates to the longstanding Berry Amendment, which requires DoD to certify that 100 percent of specialty metals used in military hardware is produced domestically. The House bill would tighten restrictions on the law, which, at least until recently, has not been strongly enforced at lower levels of the DoD supply chain. In a position statement, the Semiconductor Industry Association says that "today

the Department of Defense and their military suppliers will be unable to find semiconductors that comply with the Berry Amendment as it is currently being applied, and they will also be unable to find companies able to comply with the provisions included in HR 5122, the House−passed version of the defense authorization bill."
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily _story.jsp?id=news/MET07116.xml

5. *July 10, U.S. Air Force* — **Air Force officials consolidate network operations.** Air Force officials have formally consolidated the service's network operations and created the Air Force Network Operations, or AFNETOPS, command structure at 8th Air Force in Barksdale Air Force Base, LA. The AFNETOPS, pronounced "AF Net Ops," Command stood up in a ceremony Wednesday, July 5. The move is part of a larger Air Force reorganization of its network operations structure designed to better support the warfighter. It puts all Air Force units charged with network operations under the command of a single commander, Lt. Gen. Robert J. Elder Jr., 8th Air Force and AFNETOPS commander. "As an Air Force asset, we need to be able to go anywhere in the world and plug into Air Force communications," Elder said. "We are working toward a point where all our systems will be interoperable, giving a huge advantage to the warfighter."
Source: http://www.af.mil/news/story.asp?id=123023090

6. *July 10, Washington Technology* — **Defense to restructure contracting in Iraq.** The Department of Defense's (DoD) Business Transformation Agency (BTA) has been charged with restructuring and transforming contracting processes and systems in Iraq. Gordon England, deputy secretary of Defense, appointed Paul Brinkley, Defense deputy undersecretary for business transformation and co−director of BTA, to direct the Task Force to Support Improved DoD Contracting and Stability Operations in Iraq. The task force will evaluate DoD business enterprise processes and systems in Iraq affecting contracting, logistics, fund distribution and financial management, and "will ensure alignment to theater commanders' goals for reconstruction and economic development," England wrote in a memo dated June 22.
Source: http://www.washingtontechnology.com/news/1_1/defense/28914−1 .html

[Return to top]

Banking and Finance Sector

7. *July 11, Websense Security Labs* — **Multiple Phishing Alert: Fraudulent "Stop Fraud Now" Program, Astoria Federal Savings, GM Card.** Websense Security Labs has received reports of several new phishing attacks. The first targets customers of Bank of America and various other banks. Users receive a spoofed e−mail message, which claims that a new security program called SFN (Stop Fraud Now) has been launched. The program claims to provide protection against cloning of credit cards and asks users to provide details, such as Social Security Number, card number, and ATM Personal Identification Number. The message provides a link to a phishing Website that requests users enter their personal information and account details. Another attack targets customers of Astoria Federal Savings, which is based in New York. Users receive a spoofed e−mail message that claims that due to new security measures the user must provide a phone number. Users are directed to verify their identities by logging on. The message provides a link to a phishing Website that asks for account and

personal information. Another attack targets customers of GM Card. Users receive a spoofed e−mail claiming that, due to new security measures, the user must verify his or her account. The message provides a link to a phishing Website that asks for account and personal information.
Screenshots: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =546
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =548
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =549
Source: http://www.websensesecuritylabs.com

8. *July 10, InformationWeek* — **FBI warns job hunters of online scams.** Job candidates should be cautious when seeking employment online, according to the FBI. The FBI has released a warning, saying it is investigating several online employment scams. Some of the cases under investigation involve fake job interviews or offers of employment that are actually ways to lure people into helping crime rings. According to the warning, fake recruiters are pretending to do background checks or set up bank accounts for direct deposit. Instead of getting a job, the candidates become victims of identity theft or owners of empty bank accounts. In other cases, job ads for correspondence managers or import/export specialists are ruses to get people to ship items "purchased illegally online" using stolen credit cards, to Nigeria and other places.
Source: http://www.informationweek.com/news/showArticle.jhtml?articl eID=190301898

[Return to top]

Transportation and Border Security Sector

9. *July 11, Associated Press* — **Woman dies in Boston tunnel ceiling accident.** A woman was killed when part of the ceiling in a Big Dig tunnel fell on a car in South Boston, and a man believed to be the driver was taken to a hospital with minor injuries, authorities said. The $14 billion Big Dig highway project, which buried Interstate 93 beneath downtown and extended the Massachusetts Turnpike to Logan Airport, has been criticized for construction problems and cost overruns that state officials have said did not compromise safety. State Police Trooper Kara England said the tunnel was shut down until state safety engineers could assess its condition after the incident. Shortly after the accident, at least three large pieces of debris, tilted slightly at one side, could be seen lying across a lane of the roadway about 100 feet from the end of the connector tunnel. There have been water leaks in parts of the tunnel system and at least one incident when smaller amounts of dirt and debris from an airshaft in another section of the tunnel system fell onto travel lanes, causing minor damage to cars. In May, prosecutors charged six current and former employees of a concrete supplier with fraud for allegedly concealing that some concrete delivered to the Big Dig was not freshly mixed.
Source: http://www.cnn.com/2006/US/07/11/bigdigdeath.ap/index.html

10. *July 11, CBS* — **Rail car leaks hydrochloric acid.** Emergency crews in Riverdale, IL, remain on the scene Tuesday, July 11, after a rail car leaked hydrochloric acid in the south suburb. No injuries were reported. Hydrochloric acid was leaking from a CSX railroad car and the Riverdale Fire Department sent a Hazmat team to the scene, according to a Riverdale Fire lieutenant. The leaking rail car is in a rail yard that is mostly unseen from the roadway, and isn’t causing any major traffic problems, he said. It was unknown immediately how long it would take to secure the scene, said the lieutenant. “It’s hard to say, they have to be careful with it,’’ he said.

Source: http://cbs2chicago.com/local/local_story_192062323.html

11. *July 11, Department of Homeland Security* — **Explosive detection technologies tested at Jersey City's Exchange Place Station.** The Department of Homeland Security (DHS), with the cooperation of the Port Authority of New York and New Jersey, will test and evaluate security equipment and operating procedures at the Exchange Place Port Authority−Trans Hudson (PATH) Station from July 13−27 as part of the Department's broader efforts to protect citizens and critical infrastructure from possible terrorist attacks. Exchange Place Station is the sixth busiest among the 13 PATH stations, transporting approximately 15,000 passengers on a typical workday. Peak rush hour brings more than 4,000 passengers per hour, compared to about 400 during slower times −− all funneled through two entrances. The testing will also provide data such as percentage of false alarms, rate of screening, delays of passengers and manpower requirements −− all of which DHS will use to determine life−cycle costs and conduct ongoing risk analyses. This test is the second phase of a rail security pilot project. In phase one, which was conducted from February 6 through March 1, 2006, bags and passengers at Exchange Place Station were screened deliberately and randomly using off−the−shelf equipment such as x−ray machines and metal detectors specifically modified for the rail transportation environment.
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0948.xml

12. *July 11, Associated Press* — **Explosions hit Mumbai commuter trains, killing at least 163.** At least 163 people were killed when blasts ripped apart commuter trains in the Indian city of Mumbai during evening rush hour on Tuesday, July 11, police said. "The death toll is 163, the total injured is 464," a Mumbai police spokesperson said. There was no immediate claim of responsibility in the eight bombings, which came in quick succession −− a common tactic employed by Kashmiri militants. The blasts came hours after a series of grenade attacks by Islamic extremists killed eight people in the main city of India's part of Kashmir. Mumbai, capital of the Maharashtra state in western India, is the country's financial center. The sprawling city, known as Bombay until 1995, has seen several bombings in the past. A series of blasts in 1993, including one that targeted the Bombay Stock Exchange, killed about 250 people and injured more than 1,000. Maharashtra Chief Minister Vilasrao Deshmukh said after an emergency state cabinet meeting in Mumbai that the city was on "high alert." Deshmukh said he spoke to Prime Minister Manmohan Singh after the blasts. Commuter transit systems have been tempting targets for terrorists in recent years, with bombers killing 191 in Madrid, Spain, in 2004, and 52 in London last year.
Source: http://www.usatoday.com/news/world/2006−07−11−india−trains_x .htm

13. *July 11, Associated Press* — **New York increases transit security after India rail bombings.** New York City increased its transit security Tuesday, July 11, sending hundreds of additional officers to patrol subways and conduct random bag searches following deadly bombings on a busy commuter rail system in India. The New York Police Department said the measures were precautionary and there had been no specific threat to New York. "We take a terror attack in any place in the world, especially one on a public transport system, as a serious warning," Mayor Michael Bloomberg said. The city's 468 subway stations serve an average 4.5 million daily riders. The Metropolitan Transportation Authority also announced increased security on its rail lines, tunnels and bridges, and in Grand Central Terminal and Pennsylvania Station. The city began random bag searches a year ago in response to the mass transit bombings in London.

Source: http://www.usatoday.com/news/nation/2006−07−11−nyc−india_x.h tm

14. *July 08, Irish Examiner (Ireland)* — **Irish airport security to be stepped up after second bomb scare.** Security at Dublin Airport will be stepped up after two bomb scares delayed 110 planes and affected 21,000 passengers in the past five days. The Dublin Airport Authority (DAA) said it will work with guards and airport police in the coming weeks to review security arrangements at the airport. A spokesperson said DAA hopes to come up with a "detailed and appropriate" plan that will ensure safety and prevent similar disruption in the future. Ryanair, which was forced to cancel nine of its flights on Friday, July 7, and 12 on Tuesday, July 4, called for an investigation into how the DAA assesses threats.
Source: http://www.irishexaminer.com/irishexaminer/pages/story.aspx−qqqg=ireland−qqqm=ireland−qqqa=ireland−qqqid=7874−qqqx=1.asp

[Return to top]

Postal and Shipping Sector

15. *July 11, KansasCityChannel* — **Camden County on alert for mailbox explosives.** The Camden (MO) County Sheriff's Department Monday, July 10, warned residents to be on alert after some mailbox explosives were found. The sheriff said at least three people in Linn Creek, MO, had their mailboxes destroyed by explosives over the weekend. The sheriff said the devices are dangerous and can be fatal.
Source: http://www.thekansascitychannel.com/news/9495537/detail.html

[Return to top]

Agriculture Sector

16. *July 11, Agence France−Presse* — **China reports new outbreak of foot−and−mouth disease.** China has reported a fresh outbreak of foot−and−mouth disease (FAMD), with 51 head of cattle affected in the nation's northwestern Qinghai province. Cattle at three farms in Qinghai's Henan County began showing symptoms of FAMD on July 1, and on July 7 they were diagnosed with foot−and−mouth disease, the agriculture ministry said. A total of 212 head of cattle were culled following the outbreak. The case is the third in Qinghai this year, and brings to nine the total number of FMD outbreaks to strike China so far in 2006.
Source: http://news.yahoo.com/s/afp/20060711/hl_afp/healthchinafarm_060711033451

17. *July 10, Associated Press* — **Canada testing animal suspected of mad cow.** The Canadian Food Inspection Agency is testing the remains of a dairy cow from Alberta suspected of having bovine spongiform encephalopathy (BSE), or mad cow disease. An initial set of tests failed to rule out the possibility the 4−year−old cow died of BSE. The agency is testing other cattle born on the same farm, in the year before and the year after the affected animal, to help determine whether the infection originated on the farm. If confirmed, it would be the seventh case of mad cow disease in Canada.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/10/AR2006071000643.html

18. *July 10, Stop Soybean Rust News* — **Soybean rust found in Georgia soybean sentinel plot.** Asian soybean rust has been found in soybeans at the sentinel plot in Attapulgus, GA, in Decatur County. This is the 25th county in the U.S. with rust in five states, and the third find in this season's soybeans. The Decatur County sample came from a soybean sentinel plot located at the University of Georgia Attapulgus Research and Education Center −− located in the southwest corner of the state and about 15 miles from Quincy, Fl, where rust has been confirmed.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=879

[Return to top]

Food Sector

19. *July 11, Associated Press* — **Imported tuna may have higher mercury level.** Many imports of canned tuna have mercury levels higher than the federal limit, according to analysis by an environmental group. Defenders of Wildlife found the highest levels of mercury in tuna from Ecuador and Mexico. The group had a laboratory test 164 cans of tuna labeled as being from Ecuador, Mexico, Costa Rica, Thailand, Malaysia, the Philippines and the U.S. Analysis of the samples found average mercury content of U.S. tuna was generally lower than imported tuna.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/11/AR2006071100315.html

20. *July 10, Reuters* — **Drug−resistant E. coli likely started in poultry.** The food−contaminating bug E. coli appears to be developing resistance to antibiotics called fluoroquinolones in chickens. The problem is arising largely because of antibiotic treatment of the animals, which forces the microbes to mutate and become resistant. Food−borne resistant E. coli can then be transmitted to humans. Action to interrupt the transmission of resistant bacteria from animals to humans may become necessary. Such measures could include "limiting antimicrobial use in food animals, adopting more hygienic food−processing and distribution practices, irradiating food, and improving kitchen hygiene." In the late 1990s, James Johnson of the University of Minnesota and colleagues obtained E. coli from 35 blood samples and 33 fecal samples from patients with food poisoning seen at a hospital in Spain. The investigators also evaluated 49 fecal specimens from chickens at three slaughterhouses in the area. They found that 30 of the human specimens and 30 of the chicken specimens were resistant to Cipro, a type of fluoroquinolone antibiotic. Resistant human isolates resembled the resistant chicken isolates in terms of virulence and their DNA sequence.
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006−07−10T172809Z_01_COL062862_RTRUKOC_0_US−E−COLI.xml&archived=False

[Return to top]

Water Sector

Nothing to report.

[Return to top]

Public Health Sector

21. *July 11, Bloomberg* — **Romania's fowl−culling stems spread of bird flu.** Romania culled almost one million fowl in May, stemming outbreaks of lethal bird flu, the U.S. Department of Agriculture (USDA) said. The H5N1 avian influenza virus was actively circulating in four of Romania's counties on June 30, compared with 18 counties in May, the USDA's Foreign Agricultural Service said.
Source: http://www.bloomberg.com/apps/news?pid=20601087&sid=a0K4uLB6 RoqM&refer=

22. *July 11, New York Times* — **New York unveils a plan to identify, and contain, a flu pandemic.** Responding to the growing threat of global illnesses like the avian flu, New York City officials announced a plan Monday, July 10, to combat a flu pandemic that could sicken millions of New Yorkers. In making the announcement, Mayor Michael Bloomberg and the city’s health commissioner, Thomas Frieden, offered a blueprint for identifying an outbreak, containing its spread and distributing scarce resources like ventilators and antiviral medications. In the city’s worst−case projection of a pandemic, roughly 2.5 million New Yorkers would become infected, resulting in more than 56,000 deaths. The response plan assumes that medications and equipment would be scarce, and that a vaccine for a newly identified virus would not become available for six to nine months. The plan emphasizes the importance of early detection to help contain the spread of the illness. Officials said that they had strengthened communications with doctors across the city, who often see the first signs of infection. In addition, the Department of Health has developed a monitoring system that can keep track of 60,000 pieces of information each day including ambulance runs, emergency room visits and pharmacy sales.
Source: http://www.nytimes.com/2006/07/11/nyregion/11flu.html?_r=1&o ref=slogin

23. *July 11, BBC News* — **Drug approved to battle superbug.** A new drug to tackle the hospital superbug Methicillin−resistant Staphylococcus Aureus (MRSA) is to be introduced in Scotland. The Scottish Medicines Consortium (SMC) has recommended the antibiotic Tygacil to treat hospital infections. The drug was approved for use by the European Commission in April, but will not yet be available in England. Trials of the drug Tygacil have shown its ability to combat certain infection strains that have become resistant to medicines, including MRSA and the E.coli bug. The antibiotic, also known as tigecycline, has been approved for restricted use in Scotland to treat complicated internal infections as well as those affecting skin and soft tissue.
MRSA information: http://www.cdc.gov/ncidod/dhqp/ar_mrsa.html
Source: http://news.bbc.co.uk/2/hi/uk_news/scotland/5167746.stm

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

24. *July 11, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity in the Eastern Pacific: As of 5:00 am EDT Tuesday, July 11, Tropical Depression 3E has been designated as Tropical Storm (TS) Bud. TS Bud is about 700 miles south of the southern tip of Baja California and is moving west−northwest at about eight mph. Maximum sustained winds are about 40 mph with gusts to about 50 mph. At this time, TS Bud is a hazard to shipping only, not to the U.S. or to any land area.
Wildfire Update: Four new large fires were reported, three in the southern California Area and one in the Rocky Mountain Area. A low pressure trough is expected to move into the Pacific Northwest as high pressure begins to weaken in the West. This will tend to shift the thunderstorm activity of the last few days eastward. California and the Pacific Northwest will also begin to cool off and see higher humidity.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat071106.shtm

25. *July 10, NBC 4 (District of Columbia)* — **Emergency drill on Potomac River reveals communication problem.** An emergency drill Monday, July 10, that included a simulated burning ship and rescuers from the District of Columbia (DC), Virginia and the U.S. Coast Guard revealed a glitch in the region's emergency response system. DC Fire and Emergency Medical Services spokesperson Alan Etter said the biggest problem they found was a failed communications patch between Alexandria, VA, firefighters and the DC fire communications center. Etter said they were able to overcome the problem because firefighters from Alexandria and DC could talk directly on the same radio band.
Source: http://www.nbc4.com/news/9491856/detail.html

26. *July 10, Mississippi Press* — **Weather watchers seek to improve hurricane forecasts.** The National Hurricane Center and the field service offices of the National Weather Service (NWS) performed their jobs very well during Hurricane Katrina, according to a recently released NWS assessment conducted in the wake of the storm. But the service assessment team that visited and talked with local Weather Service officials, state and local emergency management personnel and mass media representatives issued 20 recommendations to improve the Weather Services' abilities in the future.
To read the full report: http://www.nws.noaa.gov/om/assessments/pdfs/Katrina.pdf
National Weather Service: http://www.nws.noaa.gov/
Source: http://www.gulflive.com/news/mississippipress/index.ssf?/base/news/1152526554234600.xml

[Return to top]

Information Technology and Telecommunications Sector

27. *July 10, Security Focus* — **Microsoft Office MSO.DLL LsCreateLine() potential code execution vulnerability.** Microsoft Office is reported to be prone to a potential code execution vulnerability. Analysis: This vulnerability occurs when the application handles a specially

crafted document. A successful attack may result in a remote compromise in the context of an affected user. Attack attempts may result in a denial−of−service condition as well.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18905/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18905/references

28. *July 10, Security Focus* — **Microsoft Internet Explorer OuterHTML redirection handling information disclosure vulnerability.** Microsoft Internet Explorer is prone to information disclosure vulnerabilities because it fails to properly enforce cross domain policies. Analysis: This issue may allow attackers to access arbitrary Websites in the context of a targeted user's browser session. This may allow attackers to perform actions in Web applications with the privileges of exploited users or to gain access to potentially sensitive information. This may aid attackers in further attacks.
For a list of vulnerable products: http://www.securityfocus.com/bid/18682/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18682/references

29. *July 10, Security Focus* — **Microsoft HLINK.DLL link memory corruption vulnerability.** Microsoft HLINK.DLL is prone to a memory corruption vulnerability. This issue is due to the library's failure to properly bounds check user supplied input before copying it to an insufficiently sized memory buffer. Analysis: Successfully exploiting this issue allows attackers to execute arbitrary machine code in the context of applications that use the affected library. This facilitates the remote compromise of affected computers. Failed exploit attempts will likely crash target applications. This issue has been shown to be exploitable through Microsoft Excel files. Other applications using the affected library may also be affected.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18500/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18500/references

30. *July 10, eWeek* — **Websense mines for malicious code with Google.** Security researchers have a brand−new tool to use to go digging for malicious executables on the Web: The Google SOAP Search API. Malware hunters at Websense's Security Labs have figured out a way to use the freely available Google API to find dangerous .exe files sitting on thousands of Web servers around the world. The Google API uses the Simple Object Access Protocol (SOAP) and Web Services Description Language (WSDL) standards to offer developers an easy way to run search queries outside of the browser and, because of the way the search engine indexes executables, Websense was able to create code to look for strings associated with malware packers. Dan Hubbard, senior director of security and technology research at the San Diego−based Web filtering software firm, said the use of the Google API started as an experiment after bloggers noticed that some Google search queries were returning .exe files.
Source: http://www.eweek.com/article2/0,1895,1986770,00.asp

31. *July 10, New York Times* — **Dell's exploding computer and other image problems.** A Dell notebook computer burst into flames last month in Osaka, Japan. Photos of the flaming and smoking notebook were posted on a technology news Website called the Inquirer on June 21. Two days later, Cindy Shaw, a securities analyst with Moors & Cabot, notified her clients about the publicity. Last Thursday, July 6, citing reports of a second smoking laptop, this one in

Pennsylvania, she advised them that "should this story also hit the mainstream press, we believe there is headline risk and potentially negative demand ramifications for Dell." Dell said its engineers examined and tested what remained of the flaming notebook computer for several days to find the source of the problem. They concluded that the fire was caused by a faulty lithium ion battery cell. Dell said that it found no pattern of battery failure and that the Pennsylvania incident publicized by the Inquirer Website was caused by a chip problem and not batteries.
Photos of the Osaka, Japan, incident: http://theinquirer.net/default.aspx?article=32550
Source: http://www.nytimes.com/2006/07/10/technology/10dell.html?n=Top%2fReference%2fTimes%20Topics%2fPeople%2fD%2fDarlin%2c%20D amon

32. *July 07, Security Focus* — **Researchers look to predict software flaws.** Using historical data, researchers at Colorado State University are attempting to build models that predict the number of flaws in a particular operating system or application. In an analysis to be presented at a secure computing conference in September, three researchers used monthly flaw tallies for the two most popular Web servers −− the Apache Foundation's Apache Web server and Microsoft's Internet Information Services server −− to test their models for predicting the number of vulnerabilities that will be found in a given code base. The goal is not to help software developers to create defect−free software −− which may be so unlikely as to be impossible −− but to give them the tools to determine where they need to concentrate their efforts, said Yashwant Malaiya, professor of computer science at Colorado State University and one of the authors of the paper on the analysis. The research could be another tool for developers in the fight to improve programmers' security savvy and reduce the number of flaws that open up consumers and companies to attack. While the number of vulnerabilities found in recent years leveled off, Web applications boosted the number of flaws found in 2005.
Source: http://www.securityfocus.com/news/11399

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of multiple vulnerabilities in Microsoft Internet Explorer (IE) 6.0. US−CERT is also aware of a public blog that will be posting new web browser bugs on a daily basis in July. US−CERT will be analyzing relevant vulnerabilities, as well as actively monitoring the site to provide additional information as it becomes available. Please review URL: http://metasploit.blogspot.com/2006/07/month−of−browser−bugs .html

US−CERT strongly recommends the following:

Review VU#159220 / Microsoft Internet Explorer vulnerable to heap overflow via the HTML Help Control "Image" property : http://www.kb.cert.org/vuls/id/159220

Disable ActiveX as specified in the following:

Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

Do not follow unsolicited links.

Review the steps described in Microsoft's document to improve the safety of your browser: http://www.microsoft.com/athome/security/online/browsing_saf ety.mspx

US−CERT will continue to update current activity as more information becomes available.

Public Exploit Code for Unpatched Vulnerabilities in Microsoft Internet Explorer

US−CERT is aware of publicly available exploit code for two unpatched vulnerabilities in Microsoft Internet Explorer. By persuading a user to double click a file accessible through WebDAV or SMB, a remote attacker may be able to execute arbitrary code with the privileges of the user. US−CERT is tracking the first vulnerability as VU#655100: http://www.kb.cert.org/vuls/id/655100

The second issue is a cross domain violation vulnerability that is being tracked as VU#883108: http://www.kb.cert.org/vuls/id/883108

Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited links.

To address the cross domain violation vulnerability (VU#883108):
http://www.kb.cert.org/vuls/id/883108

Disable ActiveX as specified in the Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Review Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

US−CERT will continue to update current activity as more information becomes available

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 25 (smtp), 50497 (−−−), 113 (auth), 445 (microsoft−ds), 24232 (−−−), 80 (www), 4672 (eMule), 135 (epmap), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.